(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000029792 A**

(43) Date of publication of application: **28 . 01 . 00**

(51) Int. Cl **G06F 12/14**

(21) Application number: **10195353**

(22) Date of filing: **10 . 07 . 98**

(71) Applicant: **HITACHI LTD**

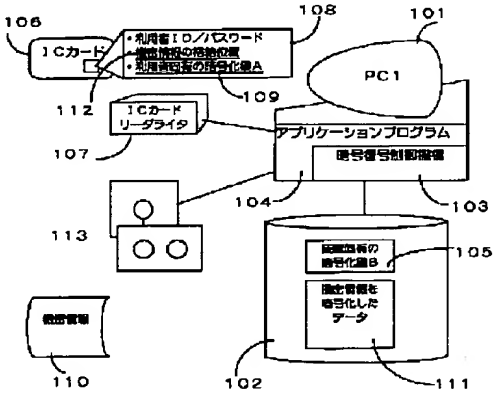
(72) Inventor: **TOMIZAWA SATOSHI**

(54) **SECRET INFORMATION STORAGE DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To improve the confidentiality by storing information on a user, information showing the storage destination of secret information, and an encoding key characteristic of the user on a small-capacity medium and generating and storing a key characteristic of the device on a hard disk.

SOLUTION: At incorporating, a key B105 characteristic of the device is generated and stored on an external storage device 102. Then the user actuates an encoding control mechanism 103 to register information 108 on the user. The contents of the information 108 of the user consist of a user ID, a password, and the encoding key A109 characteristic of the user. Then the user specifies desired secret information 110 to be concealed. An encoding control mechanism 103 reads the secret information 110 out and encodes it with a key A109 characteristic of the user. Consequently, a file obtained by further encoding the obtained file with the encoding key 105 characteristic of the device is written to a location such that the user specifies on the external storage device of the device. The location that the user specifies is written as a storage location 112 of the confidential information to an IC card 106.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－29792
（P2000－29792A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｃ　５Ｂ０１７

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平10－195353

(22)出願日　平成10年７月10日(1998.7.10)

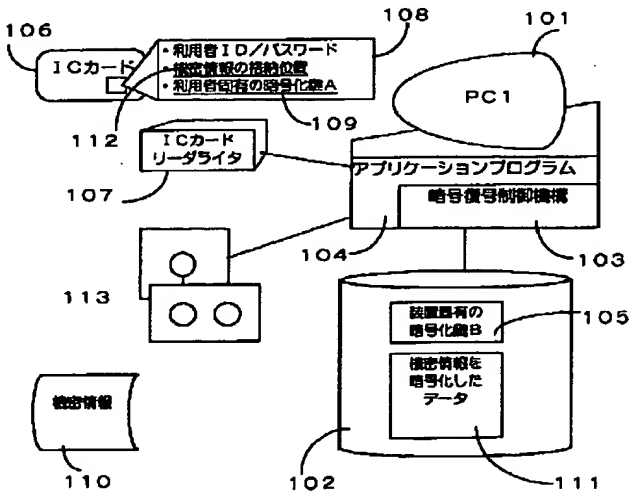
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　富澤　智
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　5B017 AA06 BA05 BA07 CA14

(54)【発明の名称】　機密情報格納装置

(57)【要約】
【課題】格納された利用者の情報と利用者の入力情報を突き合わせて正しい時、機密情報にアクセスするための鍵を取出す方法などでは、利用者の情報と機密情報または機密情報にアクセスする鍵が同一の媒体に格納され悪意の第三者により媒体自体が盗まれた場合、総当たり的な方法で利用者の機密情報または機密情報にアクセスするための鍵を取出すことができる危険性がある。
【解決手段】本発明では機密情報を格納する時に利用者固有の鍵と装置固有の鍵とを使用することにより、暗号化し、より機密性の高い情報の格納方法を提供するものである。

図１



1

【特許請求の範囲】

【請求項１】装置固有の鍵を生成し保管する手段と、利用者の認証が正常に行われた時のみ小容量媒体に格納された鍵と、装置固有の鍵を取り出す手段と、それらの鍵を用いて機密情報を２重に暗号化し外部記憶装置に格納する手段と、これらの手段を制御する機構を備えることにより機密性を高めることを特徴とする機密情報格納装置。

【請求項２】装置固有の鍵を生成し保管する手段と、利用者の認証が正常に行われた時のみ小容量媒体に格納された鍵と、装置固有の鍵を取り出す手段と、それらの鍵を用いて２重に暗号化された外部記憶装置にある機密情報を復号する手段と、これらの手段を制御する機構を備えることにより機密性を高めることを特徴とする機密情報格納装置。

【請求項３】上記に加え、小容量媒体を用いた利用者の認証が正常に行われた時のみ装置固有の鍵を取り出し復号する手段と、装置固有の鍵で複合した機密情報（利用者の鍵で暗号化した機密情報）を媒体に書き込む手段と、利用者の認証が正常に行われた時のみ装置固有の鍵を取り出し媒体に書き込まれた利用者の鍵で暗号化された機密情報（装置固有の鍵で複合した機密情報）を装置固有の鍵で暗号化し外部記憶装置に格納する手段を備えることにより機密情報を不用意に複写されることを防ぐことを特徴とする請求項１又は２記載の機密情報格納装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータの機密情報を保管する方法に関し、特に機密情報を格納する為の比較的容量の少ない携帯性に優れた媒体（ＩＣカードなど）と比較的容量の大きい媒体（ハードディスクなど）を用いることにより機密情報を安全に格納・保管する方法に関する。

【０００２】

【従来の技術】従来の方法ではＩＣカードあるいはフロッピーディスク等の比較的容量の少ない運搬可能な媒体にユーザ情報（ユーザＩＤ、パスワードなど）を格納し、利用者により入力された利用者情報と突き合わせチェックを行うことにより、当該媒体に格納された機密情報にアクセス可能とすることで機密情報のアクセスを制限していた。あるいは同様の方法により当該媒体に格納された暗号鍵を取り出し機密情報を復号することにより機密情報へのアクセスを可能としている。

【０００３】また別の方法としては利用者情報の一部（パスワードなど）をネットワークで接続された別のコンピュータに持たせることにより利用者情報の全部が盗まれることを回避しているが、インターネットのようなオープンなネットワーク上では通信中に悪意の第３者に盗聴される危険性を回避できないため盗聴されない為に暗号化技術などを用いる必要がある。

2

【０００４】

【発明が解決しようとする課題】かかる従来の方法においては次のような課題がある。すなわち①従来の方法では利用者情報と機密情報を同一の媒体に格納するため悪意を持った第３者に媒体ごと盗まれる危険性を考慮されておらず、その場合総当たり的な方法により機密情報あるいは機密情報にアクセスする為の鍵が盗まれてしまう。②利用者情報の一部（パスワードなど）をネットワークで接続された別のコンピュータに持たせることにより利用者情報の全部が盗まれることを回避する方法ではインターネットのようなオープンなネットワーク上では通信中に悪意の第３者に盗聴される危険性を回避できない。また盗聴されない為に通信プロトコル上の暗号化技術などを用いる必要がある。

【０００５】

【課題を解決するための手段】本発明は、比較的容量の小さい運搬の容易な媒体Ａ（例：ＩＣカード、フロッピーディスク）に利用者の情報（利用者ＩＤ、パスワード）及び機密情報の格納先を示す情報、利用者固有の暗号化鍵Ａを格納し、ハードディスク内に装置固有の鍵を生成して保有することにより、利用者が保管している媒体Ａと利用者により入力される情報とハードディスク内のマシン固有の鍵とハードディスク内の暗号化された機密情報の全てが正当であった場合のみ機密情報をアクセス（閲覧、利用、変更）可能とする。

【０００６】まず当該装置に対して利用者（もしくはプレインストールの場合、出荷元のメーカ）がソフトウエアを組み込む手順の中でに装置固有の暗号化鍵Ｂを作成しハードディスクに保管する。装置固有の鍵の作り方は組み込まれた日付時刻やハードウエア固有のアドレス情報、あるいは乱数を用いて他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【０００７】次に利用者の情報を登録する手順の中で利用者固有の鍵Ａを作成し利用者情報とともに、携帯性の優れた媒体Ａに格納する。利用者固有の鍵の作り方は利用者が登録された時刻や利用者の情報の一部（パスワード）、あるいは乱数を用いて他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【０００８】これらの２つの鍵を用いて機密情報は二重に暗号化して保管される。暗号化の手順としては利用者固有の鍵Ａによる暗号化、装置固有の鍵Ｂによる暗号化の順に行う。この理由は、利用者の鍵のみで暗号化した場合はハードディスク内の機密情報のファイルを複写し、当該装置に組み込まれたソフトウエアと同様のソフトウエアが組み込まれた別の装置において、総当たり的な方法により機密情報へのアクセスが可能になることを考慮している。

【０００９】また、ハードディスクの故障を考慮した場合、機密情報を別の媒体に複写する必要があるが、媒体

Ａを用い利用者情報が正しく入力された時のみ、鍵Ｂの復号化処理を行った出力ファイルを複写先の媒体に格納する機能を持たせる。複写先の媒体から別の装置のハードディスクに格納するには、媒体Ａを用いて利用者登録した後、媒体Ａと利用者の正当な入力があった時、初めて装置固有の鍵で暗号化してハードディスクに格納する機能により実現する。

【００１０】

【発明の実施の形態】以下本発明実施の具体的方法を示す。

【００１１】図１は本発明を適用する装置とその構成を示している。以下では携帯性に優れた比較的容量の小さい媒体をＩＣカード、装置本体に固定的に接続される外部記憶装置をハードディスクとして記述する。本発明において、暗号化制御機構１０３はコンピュータ装置１０１の外部記憶装置１０２にアプリケーションプログラム１０４に含まれて組み込まれる。例えばアプリケーションプログラムは電子証明書を必要とする電子商取引のクライアントなどが考えられ、機密情報は電子証明書などが想定できる。

【００１２】組み込みの際には、装置固有の鍵Ｂ１０５を作成し外部記憶装置１０２に格納する。装置固有の鍵Ｂ１０５の作り方は組み込まれた日付時刻やハードウエア固有のアドレス情報、あるいは乱数を用いて、他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【００１３】次に利用者が暗号化制御機構１０３を起動し利用者の情報を登録する。このとき暗号化制御機構１０３はＩＣカードリーダライタ１０７により、初期化されたＩＣカード１０６内に利用者の情報１０８を書き込む。利用者の情報１０８の内容は利用者ＩＤ／パスワード、利用者固有の暗号化鍵Ａ１０９である。次に利用者が隠蔽しようとする機密情報１１０を指定する。

【００１４】これは多くの場合外部媒体１１２により読み込まれる。暗号化制御機構１０３は機密情報１１０を読取り利用者固有の鍵Ａ１０９により暗号化する。この結果、得られたファイルを更に装置固有の暗号鍵１０５により暗号化した結果得られたファイルを装置の外部記憶装置内の利用者が指定した位置に書き込む。利用者が指定した位置はＩＣカードの中に機密情報の格納位置１１２として書き込まれる。

【００１５】以下、それぞれの処理の詳細を説明する。図２にアプリケーションプログラム１０４のインストール処理のフローを示す。プログラムのインストールを開始すると通常のインストールと同様にプログラムの組込み２０１を行う。２０１には必要なディレクトリの作成、必要なプログラムファイル等の圧縮解凍および複写、プログラム動作用環境変数の設定、レジストリの設定等が含まれる。

【００１６】２０１が終了した後、装置固有の暗号鍵Ｂの生成２０２、鍵Ｂのハードディスクへの格納２０３を行いインストール処理を終了する。図３は利用者登録処理の流れを示している。まず利用者情報の読込み（利用者ＩＤ）３０１、利用者情報の読込み（パスワード）３０２を行う。これらは利用者による画面入力を読取る方法で実施する。

【００１７】次にＩＣカードを読取り３０３、データが既に存在する場合は初期化してよいかどうかを利用者に判断させる（３０４，３０７）。その後利用者固有の暗号鍵Ａを生成３０５し、利用者情報、暗号化鍵ＡをＩＣカードに書き込む。図４は機密情報の格納処理１を示す。機密情報格納処理１は全く機密情報が暗号化されていない状態から暗号化されハードディスクに格納されるまでの処理である。

【００１８】まず利用者情報、ＩＣカードの読込み（４０１，４０２）利用者の入力が正しいかを判定し４０３、正しければ機密情報の読込み４０４、ＩＣカードから暗号化鍵Ａを取出し４０５、暗号化鍵Ａで機密情報を暗号化４０６する。

【００１９】次にハードディスクから装置固有の暗号化鍵Ｂを取出し、鍵Ａで暗号化された機密情報をさらに暗号化鍵Ｂで暗号化４０８する。最後に暗号化された機密情報の格納位置を利用者に問合わせ４０９、指定された格納位置情報をＩＣカードに書き込む４１０とともに暗号化した機密情報を指定された格納位置に格納４１１する。なお、利用者情報の入力が正しくなく規定回数を超えた誤入力があった場合は処理を中止する（４１２，４１３）。

【００２０】図５、図６は上記で格納された暗号化された機密情報を別の媒体に複写する処理の手順と同様の機能がインストールされた別の装置のハードディスクにに媒体を経由して機密情報を格納する方法を示す。図５の複写処理では、まず利用者情報の読込み５０１、ＩＣカードの読込み５０２を行い入力が正しかった場合５０３は、ＩＣカードから格納位置情報を読取り５０４、格納位置に格納された暗号化された機密情報を読込み５０５、暗号化鍵Ｂを取出し５０６、機密情報の暗号化鍵Ｂによる復号化５０７を行う。次に複写先の位置を利用者から画面入力させ５０８、鍵Ｂで複合された機密情報（鍵Ａで暗号化されている）を複写先に指定された媒体に格納５０９する。利用者情報の入力誤りは図４と同様（５１０，５１１）。

【００２１】図６の機密情報格納処理２（別の装置への格納処理）では、まず利用者情報の読込み６０１、ＩＣカードの読込み６０２、利用者の入力が正しかった場合６０３には、入力元ファイルの位置情報を利用者に入力させ６０４、暗号化鍵Ｂで復号化された機密情報（暗号化鍵Ａで暗号化されている）を入力元ファイルの位置から読込み６０５、暗号化鍵Ｂ’を取出し６０６（鍵Ｂ’：別の装置であるため鍵Ｂと異なることを意味す

る）、鍵Ｂ’により暗号化６０７する。

【００２２】次に格納先の位置を利用者に入力させ６０８、暗号化した機密情報を指定された格納先に格納する６０９とともにＩＣカード内の機密情報の格納位置情を書き換える６１０。利用者情報の入力の誤りは図４の説明と同様である（６１１，６１２）。

【００２３】

【発明の効果】以上述べたように、本発明によれば装置内に格納された利用者の機密情報をＩＣカードなどの運搬の容易な媒体と正当な利用者による入力が揃わなければ取り出すことができないよう保護することができ、また装置の故障にそなえ利用者が機密情報を別の媒体に簡易に複写できながら他の不正利用者による機密情報の複写を防止できる手段を提供できる。

【図面の簡単な説明】

【図１】本発明の機密情報格納装置の動作する装置の形態図。

【図２】本発明のソフトウエアのインストール処理の具体的フローチャート図。

【図３】本発明のソフトウエアにおける利用者登録処理の具体的フローチャート図。

【図４】本発明の機密情報格納処理１の具体的フローチャート図。

【図５】本発明の機密情報複写処理の具体的フローチャート図。

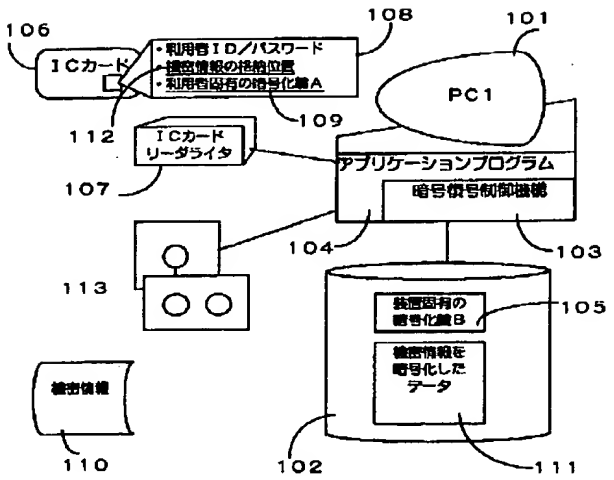
【図６】本発明の機密情報格納処理２の具体的フローチャート図。

【符号の説明】

１０１…本発明のソフトウエアが動作するコンピュータ装置、１０２…装置に接続された外部記憶装置、１０３…本発明の機能となる暗号復号制御機構、１０４…暗号復号制御機構を含むアプリケーションプログラム、１０５…装置固有の暗号化鍵Ｂ、１０６…利用者の情報などを格納するＩＣカード、１０７…ＩＣカードリーダライタ、１０８…ＩＣカードに格納された利用者固有の情報、１０９…利用者固有の暗号化鍵Ａ、１１０…隠蔽したい機密情報、１１１…暗号化され格納された機密情報、１１２…機密情報の格納位置情報、１１３…入出力媒体（ＦＤ、ＤＡＴなど）、２００…プログラムインストール処理開始、２０１…プログラムの組込み、２０２…装置固有の鍵Ｂの生成処理、２０３…鍵Ｂのハ＊ードディスクへの格納、３００…利用者登録処理開始、３０１…利用者情報の読込み（利用者ＩＤ）、３０２…利用者情報の読込み（パスワード）、３０３…ＩＣカードの読取り、３０４…ＩＣカードに登録済みデータがあるかどうかの判定、３０５…暗号化鍵Ａの生成、３０６…利用者情報、暗号化鍵ＡのＩＣカードへの書込み、３０７…ＩＣカードを初期化してよいかの判定、４００…機密情報格納処理１開始、４０１…利用者情報の読込み、４０２…ＩＣカードの読取り、４０３…利用者の入力が正しいかどうかの判定、４０４…機密情報の読込み、４０５…ＩＣカードからの暗号化鍵Ａの読込み、４０６…暗号化鍵Ａによる暗号化処理、４０７…ハードディスクから暗号化鍵Ｂの取出し、４０８…暗号化鍵Ｂによる暗号化処理、４０９…格納位置情報の利用者からの入力読込み、４１０…格納位置情報のＩＣカードへの書込み、４１１…格納位置への暗号化された機密情報の格納、４１２…誤り回数カウンタへ１を足す処理、４１３…カウンタ回数判定、５００…機密情報格納処理１開始、５０１…利用者情報の読込み、５０２…ＩＣカードの読取り、５０３…利用者の入力が正しいかどうかの判定、５０４…ＩＣカードから格納位置情報の読込み、５０５…暗号化された機密情報の読込み、５０６…ハードディスクから暗号化鍵Ｂの取出し、５０７…暗号化鍵Ｂによる復号処理、５０８…複写先情報の利用者からの入力読込み、５０９…暗号鍵Ｂで復号された機密情報（鍵Ａで暗号化されている）の複写先への格納、５１０…誤り回数カウンタへ１を足す処理、５１１…カウンタ回数判定、６００…機密情報格納処理１開始、６０１…利用者情報の読込み、６０２…ＩＣカードの読取り、６０３…利用者の入力が正しいかどうかの判定、６０４…入力元情報の利用者からの入力読込み、６０５…暗号鍵Ｂで復号された機密情報（鍵Ａで暗号化されている）の入力元からの読込み、６０６…ハードディスクからの暗号化鍵Ｂ’の取出し、６０７…暗号化鍵Ｂ’による暗号化処理、６０８…格納位置情報の利用者からの入力読込み、６０９…ＩＣカードの格納位置情報の書換え、６１０…格納位置への暗号化された機密情報の格納、６１１…誤り回数カウンタへ１を足す処理、６１２…カウンタ回数判定。

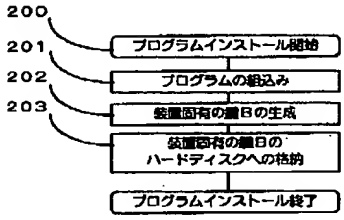
【図１】

図1



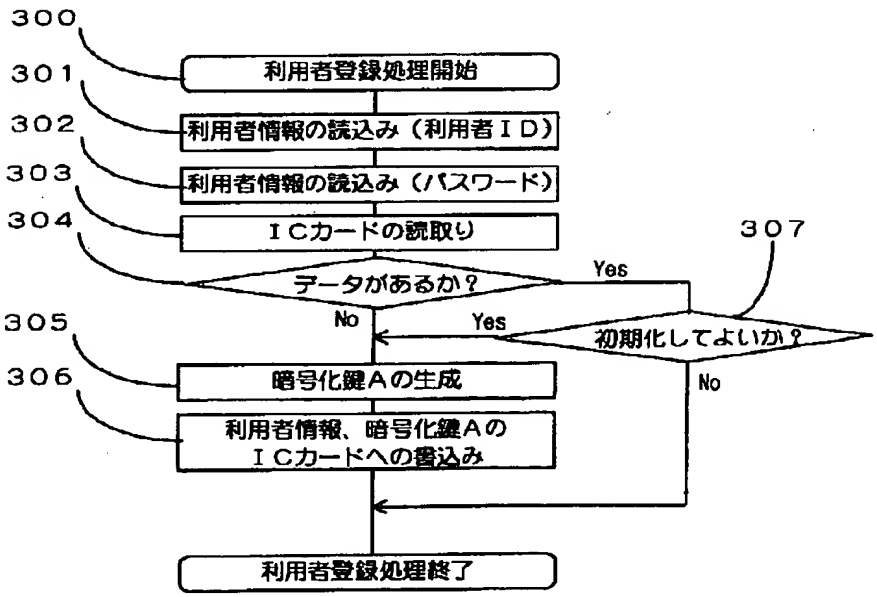
【図２】

図2



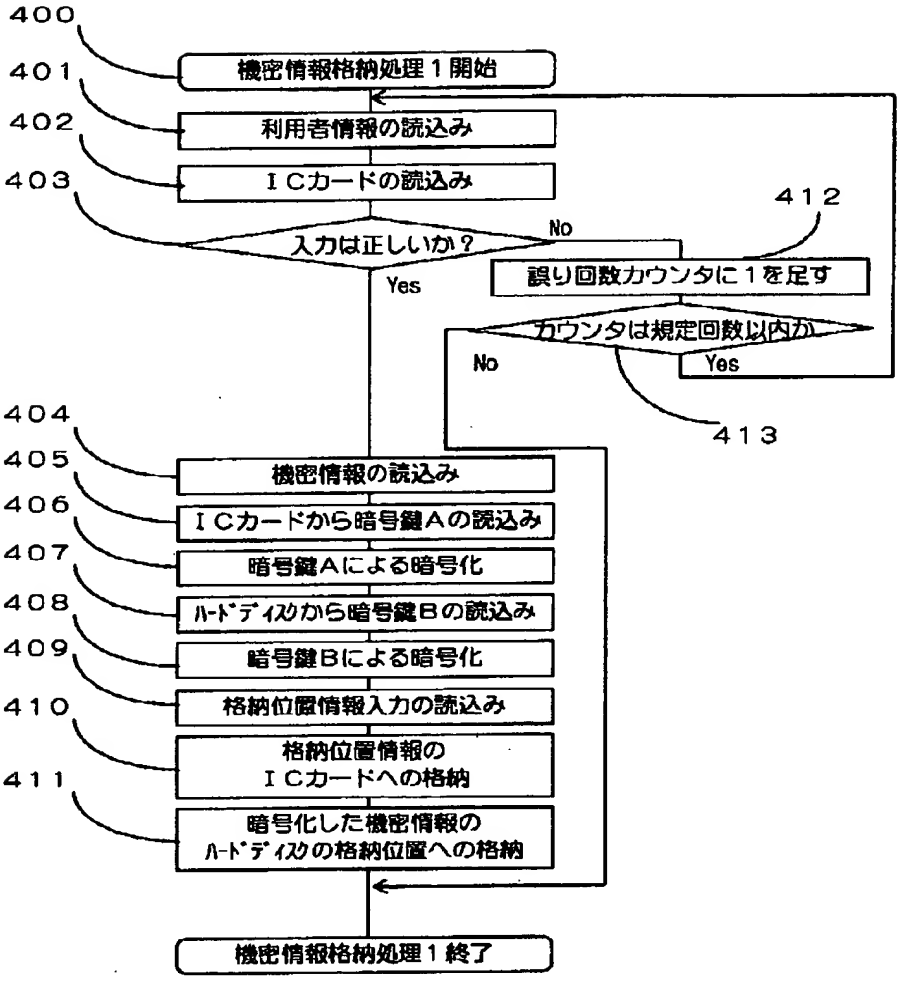
【図３】

図３



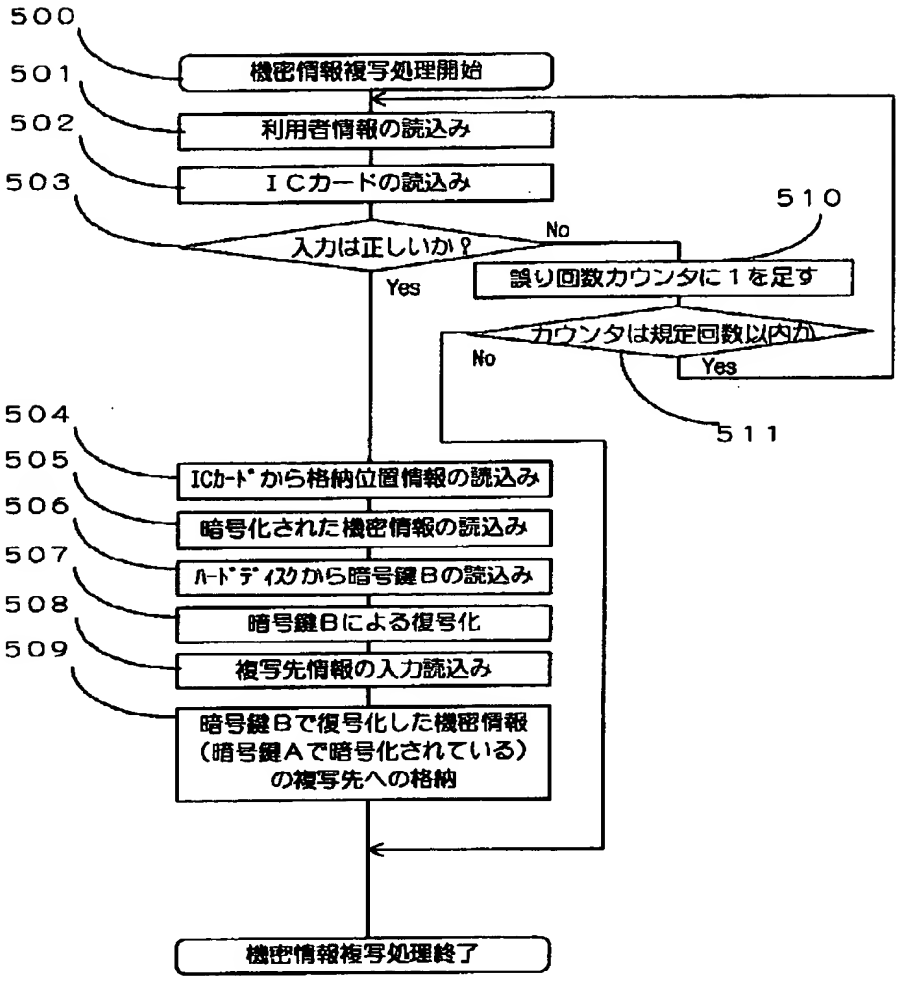
【図４】

図４


400
機密情報格納処理１開始
401
利用者情報の読込み
402
ＩＣカードの読込み
403
入力は正しいか？
No
Yes
412
誤り回数カウンタに１を足す
カウンタは規定回数以内か
No
Yes
413
404
機密情報の読込み
405
ＩＣカードから暗号鍵Ａの読込み
406
暗号鍵Ａによる暗号化
407
ﾊｰﾄﾞﾃﾞｨｽｸから暗号鍵Ｂの読込み
408
暗号鍵Ｂによる暗号化
409
格納位置情報入力の読込み
410
格納位置情報の
ＩＣカードへの格納
411
暗号化した機密情報の
ﾊｰﾄﾞﾃﾞｨｽｸの格納位置への格納
機密情報格納処理１終了

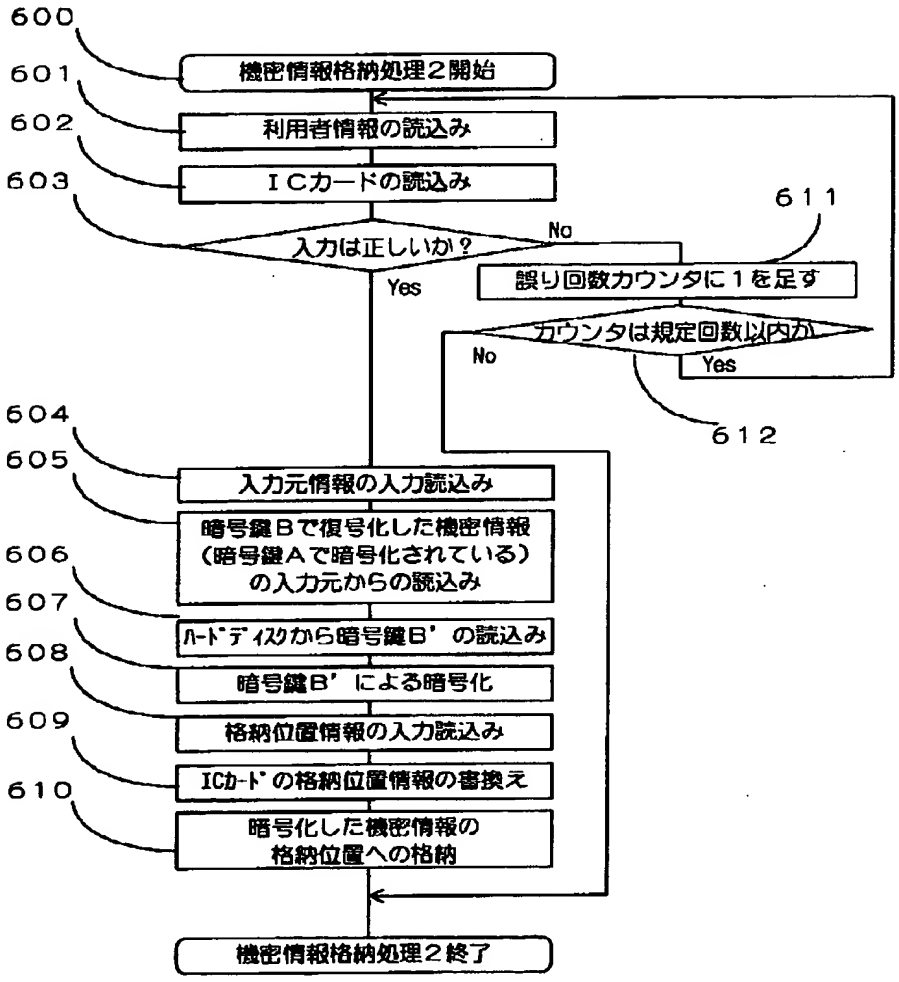
【図５】

図５


500
機密情報複写処理開始
501
利用者情報の読込み
502
ＩＣカードの読込み
503
入力は正しいか？
No
Yes
510
誤り回数カウンタに１を足す
カウンタは規定回数以内か
No
Yes
511
504
505
ICｶｰﾄﾞから格納位置情報の読込み
506
暗号化された機密情報の読込み
507
ﾊｰﾄﾞﾃﾞｨｽｸから暗号鍵Ｂの読込み
508
暗号鍵Ｂによる復号化
509
複写先情報の入力読込み
暗号鍵Ｂで復号化した機密情報
（暗号鍵Ａで暗号化されている）
の複写先への格納
機密情報複写処理終了

【図６】

図６


600
機密情報格納処理２開始
601
利用者情報の読込み
602
ＩＣカードの読込み
603
入力は正しいか？
No
Yes
611
誤り回数カウンタに１を足す
カウンタは規定回数以内か
No
Yes
612
604
605
入力元情報の入力読込み
暗号鍵Ｂで復号化した機密情報
（暗号鍵Ａで暗号化されている）
の入力元からの読込み
606
607
ﾊｰﾄﾞﾃﾞｨｽｸから暗号鍵Ｂ’の読込み
608
暗号鍵Ｂ’による暗号化
609
格納位置情報の入力読込み
610
ICｶｰﾄﾞの格納位置情報の書換え
暗号化した機密情報の
格納位置への格納
機密情報格納処理２終了